Meeting Minutes

U.S. Government Facial Recognition (FR) Legal Series
FORUM IV: *Exploring Public Perceptions of Facial Recognition Technology*
Sponsored by the Federal Bureau of Investigation's (FBI) Biometric Center of Excellence (BCOE), in conjunction with the National Institute of Justice (NIJ)

Date: June 11, 2012
Location: FBI Headquarters, J. Edgar Hoover Building, Washington DC
Attendees: See Appendix

Welcome | Mr. William Casey, Program Manager, FBI BCOE

- Mr. Casey welcomed participants to the fourth forum of the series. He thanked the speakers, forum co-sponsor, and several others who assisted in organizing the forum. He announced that the forum series has won several awards.

Mr. Casey introduced Dr. Mark Greene.

Welcome | Dr. Mark Greene, Biometric Program Manager, NIJ

- Dr. Greene welcomed the attendees. He remarked that the FR series has been relevant and thought-provoking and noted the interagency collaboration that the forum series has fostered.

Dr. Greene introduced Jennifer McNally

Forum Preview and Opening | Ms. Jennifer F. (Alkire) McNally, Management and Program Analyst, FBI BCOE and Forum Strategist

- After welcoming the attendees and reviewing several housekeeping issues, Ms. McNally reviewed the conditions that gave rise to the series; namely, a lack of law and policy expressly governing FR technology and a lack of accurate information by the public about the capabilities and limitations of FR technology and its use by the government.
- Failure to address these issues will prevent the effective use of FR technology for legitimate law enforcement and national security purposes and put individuals' privacy rights and civil liberties at risk. It also leaves the technology vulnerable to potentially detrimental court decisions and/or legislation that may occur as a response to the perception of an imperfect technology with inadequate safeguards.
- The purpose of the series has been to bring together members of federal law enforcement, intelligence, homeland security, and military agencies who are using or may in the future use

FR technology, initiate dialogue about its uses and challenges to its uses, explore the current legal and policy landscape, analyze the issues that future policy must address to more effectively use FR technology, examine the privacy and civil liberties considerations, and explore the factors that influence the public's perceptions of FR technology. The end goal is to inform inter- and intra-agency policy development.

- As a result of the series, a white paper will be produced expounding on the issues raised through the discussions. It will outline legal and societal considerations for FR technology policy development.
- The series is not intended to drive consensus on policy issues or address technical issues.

Ms. McNally introduced Chief Chris Moore.

State and Local Law Enforcement Perspectives of FR | Chief Chris Moore, San Jose Police Department

- Technology is an important policing tool, particularly in an economic environment where officers are being laid off; however, technology is expensive, so it must work effectively and reliably to justify the expense.
- To ensure public trust, two conditions must be met: First, policies governing the technology must be in place before the technology is implemented. Second, the purpose of the technology and policies safeguarding data and protecting individuals' civil liberties must be clearly communicated to the public.
- Body-mounted cameras (audio and video) on police officers will likely be deployed in the next several years to counter claims of police misconduct. Prior to deployment, policies must be developed to guide, for example, under what conditions collection will take place, how images will be securely transmitted, where and for how long massive amounts of data will be stored, who may access the data, and whether and how FR technology may be used on the images.
- Automated license plate reader (LPR) technology helps solve crime, but it presents similar policy challenges, such as the appropriate retention period for license plate images.
- There seems to be a general public acceptance of government cameras being present in places such as public transportation and courthouses, but not everywhere. Privately-owned cameras are more prevalent, and images collected on them may be obtained by law enforcement.
- Before facial images are captured, it is critical to clearly communicate to the public what is being captured, why it is being captured, and the rules being followed to safeguard the information. Public messaging must be done prior to deployment to engender public trust and support.
- Policy development must involve a public input process.
- The "realignment" initiative in California, in which people are removed from parole and set free, has increased the need for law enforcement technology.

After a break, Ms. McNally introduced Judge Frederic N. Smalkin

Judicial Impressions of FR and Recommendations from the Bench | Chief Judge Frederic N. Smalkin, U.S. District Court, D.Md. (Ret.)

- The debate between technology and privacy/civil liberties is not a new one. Voice recorders in airplane cockpits were also once viewed negatively by pilots and unions; however, after they proved useful in saving lives, resistance subsided.
- There is presently no case law specific to FR technology.
- Policy should be developed to address issues of collection and utilization.
- LPR technology can be analogized to FR technology. As such, guidance pertaining to LPR may be useful to develop guidance for FR technology.
    - The Fourth Amendment does not prohibit LPR.
    - National Policing Improvement Agency (NPIA) in England compiled practice advice on the use of automated LPR technology. It provides a conversational, straightforward way to address public concerns.
    - LPR records are subject to public disclosure under state and federal Freedom of Information Act (FOIA) requirements, with a law enforcement exception.
- In the U.S., what is not prohibited by law is generally permitted.
- A 2011 article in the University of Illinois *Journal of Law, Technology and Policy* discussing the "digitally efficient investigative state" noted that the public's concern about FR technology is primarily a factor of the false positive matches it produces, rather than the potential privacy and civil liberties implications.
- Public relations are critical. The government must convince the public that it is not interested in monitoring the average citizen's actions but, rather, in monitoring criminals' actions and otherwise protecting the public.
- <u>Collection issues:</u>
    - Earlier this year, the Maryland Court of Appeals found the routine collection of a DNA sample from arrestees to be unconstitutional under the Fourth Amendment. How might this logic predict a court's analysis of FR technology? How is FR technology similar to or distinct from fingerprints in a similar context?
    - Facial images must not be collected in a way that infringes on one's First Amendment rights (e.g., mounting a camera at the entrance of a mosque).
- <u>Access issues:</u>
    - Access to collected and stored facial images should be justified and documented, with a human screener deciding whether an image may be accessed depending on a predetermined set of criteria.
- <u>Records Retention issues:</u>
    - Statutes of limitations for particular crimes may guide retention period policy development. In Maryland, there is no statute of limitations for a felony and a one year statute of limitations for a misdemeanor. LPR records may be retained for one year in Maryland.
- <u>Utilization of FR technology at trial:</u>
    - Modern juries expect to see tangible evidence, such as photos and video.
    - Expert testimony is required per the *Daubert/Frye* standards.
    - A primary purpose of the *Daubert/Frye* standards is to throw out junk science. One indicator of junk science is a large number of false positive matches. FR

technology will need to mature before it satisfies the reliability and general acceptance requirements.
  - A University of Louisville Law Review article indicates that conclusions based on FR technology should be used only as exculpatory evidence.

Ms. McNally introduced Mr. James Loudermilk

2011 "The National Biometrics Challenge": A Call for Informed Policy Development | Mr. James Loudermilk, Co-Author and Senior Level Technologist, FBI

- In 2006, the National Science and Technology Council (NSTC) wrote the initial National Biometric Challenge document. Subsequently, 83% of federal research funding was applied to the priorities listed in the document. While privacy was a significant consideration in developing the priorities, a privacy research agenda was not developed.
- The National Biometric Challenge document was updated in September 2011. Many of the issues identified in the 2006 document have been addressed but none has been resolved.
- FR is an area in need of algorithm improvement, increased interoperability, and public education, as are other biometric modalities including finger and palm prints, iris, voice, and DNA.
- FR technology has progressed, but false positives remain a concern with large volumes of data. A goal is to reduce error rates by half every two years.
- Spending on biometric systems amounts to over $1 billion per year, underscoring the need for policy development.
- Privacy, civil rights, civil liberties, and anonymity were identified as major issues requiring policy development.
- The privacy research agenda in the 2011 document includes developing an understanding of the public's notions of privacy as it relates to biometric technologies.

The forum broke for lunch. When the group reconvened after lunch, Ms. McNally introduced Dr. Lisa Nelson.

Public Perceptions of FR: Research Conclusions | Dr. Lisa S. Nelson, J.D., Ph.D., Associate Professor, Graduate School of Public and International Affairs and Philosophy of Science Department Fellow, University of Pittsburgh; Author of *America Identified: Biometric Technology and Society*

- Emerging technologies have become user-centric. The public not only reacts to and uses technology, but public perceptions of technology drives development.
- As part of a National Science Foundation grant, Dr. Nelson conducted a national survey of 1000 people and held subsequent focus groups to develop a composite of the public's perceptions of and attitudes toward the use of biometrics, including FR technology, for identification purposes.
- The public's view of biometric technologies is less dichotomous and, therefore, more complicated than that of privacy and civil liberties advocacy groups.

- Privacy often means different things for different people. Public perceptions of privacy are influenced by values and assumptions that often differ from legal guarantees.
- When people were asked how they feel about the use of biometrics for identification as compared to other forms of identification (social security number, date of birth, etc.), privacy was only one concern they expressed. Anonymity, appropriateness of government intervention/paternalism, and trust and confidence in government are additional concerns.
    - Anonymity: Anonymity refers to one's ability not to be recognized and to maintain a meaningful degree of independence from the government. As a general premise, people do not want to be watched; however, people want to be secure. The tipping point is often unclear.
    - Paternalism: Although people do not want government intervention in all aspects of their lives, they do want the government to protect them in circumstances where individuals do not have sufficient information to know or resources to effectively handle threats such as terrorism and identity theft.
    - Trust and confidence: Where trust and confidence in a public institution exists, people are more willing to support government use of emerging technologies such as FR and willingly give up personal information.
- The word "privacy" is often used to include considerations of anonymity, paternalism, and trust/confidence.
- The justification for a government need for personal information is very relevant to people's willingness to provide it. Self-interest is a driving factor. Where people perceive a benefit to providing personal information, they are much more willing to do so.
- Specific justification for government surveillance, such as for public safety when entering a government building or airport, is more palatable to the public than a general justification, such as "for security purposes."
- It is imperative to successfully communicate to the public the government's reasoning of the benefits of FR technology and other biometrics before something goes wrong. This will enable the government to act in a paternalistic manner where appropriate. The failure to do so will result in decreased trust and confidence in government.
- How can public trust in government be developed?
    - The public looks to law and policy to instill their confidence in government.
    - Policy serves as a stand-in for human interaction and personal trust. According to research, the public trusts the medical and financial institutions because people are familiar with their personal information/privacy policies: HIPPA and the Gramm-Leach-Bliley Act, respectively. A HIPPA statement is routinely provided to people at medical appointments, and a Gramm-Leach-Bliley Act statement is a standard part of the paperwork provided to customers at the time the relationship is established and annually thereafter.
    - Interestingly, the effectiveness of these policies in protecting information privacy is less a factor of public trust than merely having been repeatedly exposed to the policies.
    - The existence of policy and public familiarity with the policy builds confidence absent a personal relationship. This underscores the need to develop policy to guide government use of FR technology and publicize the policies and reasons for them clearly and frequently to the public.

After a break, Ms. McNally reintroduced Dr. Nelson.

Pulling it All Together: A Formula for Policy Development | Dr. Lisa S. Nelson, J.D., Ph.D., Associate Professor, Graduate School of Public and International Affairs and Philosophy of Science Department Fellow, University of Pittsburgh; Author of *America Identified: Biometric Technology and Society*

- Dr. Nelson led an interactive session in which the Fair Information Practice Principles (FIPPs) were synthesized with public perception research in response to issues of concern with FR technology as they have been articulated by privacy and civil liberties groups. The purpose of the exercise was to develop practice guidelines that incorporate basic legal standards (FIPPs) and public opinion as they apply to specific issues. To facilitate the exercise, Dr. Nelson presented a matrix with the FIPPS listed across the top and the issues of concern listed down the side.
- Some of the guidelines are as follows:
    - Individual consent shifts responsibility to the individual to perceive potential problems with a particular use of information and effectively handle a problem when it occurs. This may be a disservice to the individual where the issues are numerous, complex, and/or require specialized knowledge.
    - Therefore, although the public generally expects to have the option of consent to capture and potential uses of personal information, people are willing to forego consent, instead trusting the government to protect their best interests where individuals do not have sufficient information about the issues and consequences to provide meaningful consent.
    - Opt-in and opt-out are impractical forms of consent for law enforcement and national security purposes but can be effective for civil applications under the right circumstances.
    - As a general rule, barring the conditions previously mentioned, the more information provided to the public about technology, the greater the public acceptance of it. Understanding of uses, limitations, and capabilities of technology contributes to public acceptance.
    - The public generally expects to receive information about the purpose of data collection and uses of data. For example, are people merely being scanned or are their facial images being recorded? If they are being recorded, what will be done with the information? The responsibility for providing this information should be on the government, not on the individual to seek out the information.
    - Individual consent is often viewed by the public as a necessary but insufficient way to ensure individual participation in decisions about one's personal information.
    - The public is more willing to accept biometric technology as a protector of privacy, anonymity, and safety than privacy and civil liberties groups generally are.
    - The public expects strong security features to be built into technology to protect data quality and integrity.
    - External auditing and other forms of accountability are key to building public trust and confidence in government use of biometric information.

Series Summary and Critical Next Steps | Ms. Jennifer F. (Alkire) McNally, Management and Program Analyst, FBI BCOE and Forum Strategist

- FR technology presents two competing interests: enhancement of public safety and a risk to privacy rights, civil liberties, and other societal values and expectations.
- Through the development of informed, well-reasoned law, policies, and procedures to govern appropriate uses and limitations of FR technology by the federal law enforcement and national security communities, FR technology may be utilized as an effective investigative identification tool while safeguarding individuals' rights and interests.
- Ideally, an application of FR technology should pass both legal and social muster. Ms. McNally presented a model demonstrating this two-pronged approach to vetting FR applications. In addition to illustrating whether an application is legally permissible and socially acceptable, it clarifies areas in need of reevaluation and/or development of legal authorities, and it helps to identify issues where increased public awareness may increase understanding and, therefore, support for the application.
- Through the series, participants have developed an understanding of the use cases, guiding authorities, and legal/policy challenges that arise through FR technology. These are necessary first steps toward effective policy development. It is critical that the series leads to informed policy development.
- Other critical next steps include, but are not limited to, engaging privacy and civil liberties advocacy groups, state and local law enforcement, international law enforcement and intelligence partners, and the private/commercial sector to promote understanding and share best practices and lessons learned, with the ultimate goal of advancing responsible use of FR technology.
- Participants expressed interest in additional legal and policy forums to be held addressing next generation DNA, voice recognition, iris, and multimodal biometrics.

Ms. McNally thanked the participants for their attendance. She reintroduced Mr. Casey for closing remarks.

Closing Remarks | Mr. Casey

- Mr. Casey thanked the audience and the presenters for their participation.

Mr. Casey introduced Mr. Ford for additional closing remarks.

Closing Remarks | Mr. William Ford, Division Director, NIJ

- Mr. Ford expressed gratitude to the FBI BCOE for hosting the series and thanked everyone for their participation.

Adjourned at 1630